2131 #4

Docket No. 216413US2S/btm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Asahiko YAMADA, et al. GAU: 2131

SERIAL NO: 09/989,072 EXAMINER:

FILED: November 21, 2001

FOR: SYSTEM, METHOD, AND PROGRAM FOR ENSURING ORIGINALITY

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2000-356239	November 22, 2000

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak
Registration No. 24,913
Joseph A. Scafetta, Jr.
Registration No. 26,803

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

09/989,072

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１１月２２日

出願番号
Application Number: 特願２０００－３５６２３９

出願人
Applicant(s): 株式会社東芝

２００１年１１月 ９日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３０９９０６４

【書類名】　特許願
【整理番号】　A000006737
【提出日】　平成12年11月22日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/00
【発明の名称】　原本性保証システム及びプログラム
【請求項の数】　4
【発明者】
【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中事業所内
【氏名】　山田　朝彦
【発明者】
【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中事業所内
【氏名】　原嶋　秀次
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】
【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　原本性保証システム及びプログラム

【特許請求の範囲】

【請求項１】　電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の発行した日時情報を付与し、これら電子署名と日時情報の組に対して第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証することを特徴とする原本性保証システム。

【請求項２】　電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証する原本性保証システムに関し、前記ユーザ装置に用いられるプログラムであって、

前記第１のユーザ装置のコンピュータを、

操作者の操作により、電子化データを作成する手段、

前記電子化データのうち、前記原本性の保証の対象となる電子化データに対して電子署名を生成する手段、

前記電子署名を前記第三者機関装置に送信する手段、

として機能させるためのプログラム。

【請求項３】　電子化データに対するユーザ装置の電子署名に対し、自己の電子署名を施して前記電子化データの原本性を保証するための原本性保証ポータルサービスを提供する第三者機関装置と、前記第三者機関装置から提供される原本性保証ポータルサービスをネットワークを介して利用するユーザ装置とからなる原本性保証システムであって、

前記第三者機関装置は、

前記ユーザ装置が登録されるテーブルと、

前記テーブルに登録されたユーザ装置に対し、予め前記原本性保証ポータルサービスを利用するためのプログラムを提供する手段と、

前記プログラムを用いてアクセスされたとき、前記アクセスしてきたユーザ装置のアクセス権限を前記テーブルを参照して確認する手段と、

前記アクセス権限の確認されたユーザ装置に対し、前記原本性保証ポータルサービスの利用を許可する手段と、

を備えたことを特徴とする原本性保証システム。

【請求項４】　請求項３に記載の原本性保証システムにおいて、

前記ユーザ装置は、

前記第三者機関装置による電子署名と前記電子化データとを送信する際に、送信先の候補として、前記テーブルの登録内容を前記第三者機関装置に要求する手段と、

前記要求に対する応答に基づき、前記テーブルの登録内容をリスト表示する手段と、

を備えたことを特徴とする原本性保証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、信頼できる第三者機関を介して文書の原本性を保証し得る原本性保証システム及びプログラムに係り、特に、第三者機関やネットワークにかかる負荷を低減し得る原本性保証システム及びプログラムに関する。

【０００２】

【従来の技術】

一般に、電子化された電子化文書をインターネットを介して交換するサービスは、電子化文書の原本性保証が困難である性質上、電子化文書の原本性が重要視される分野には普及が妨げられて来ている。

【０００３】

しかしながら、近年、暗号技術の発展とともに、原本性を保証する技術が実現され始めたことに伴い、原本性保証技術を実装した原本性保証サービスが使用され始めている。

【０００４】

この種の原本性保証サービスは、信頼できる第三者機関ＴＴＰ（Trusted Third Party）の計算機に電子化文書を送信することにより、第三者機関ＴＴＰに原本性を保証させる方式を基本的な技術としている。なお、以下の明細書中、第三者機関ＴＴＰは、組織そのものではなく、第三者機関ＴＴＰに運営されるサーバ

装置等の計算機を意味する。

【０００５】

【発明が解決しようとする課題】

しかしながら以上のような原本性保証システムでは、第三者機関ＴＴＰを経由して電子化文書を交換するため、第三者機関ＴＴＰへの電子化文書の送信が集中した場合、第三者機関ＴＴＰや、第三者機関ＴＴＰまでの間のネットワークに対し、負荷がかかる問題がある。

【０００６】

本発明は上記実情を考慮してなされたもので、第三者機関やその間のネットワークにかかる負荷を低減し得る原本性保証システム及びプログラムを提供することを目的とする。

【０００７】

【課題を解決するための手段】

第１の発明は、電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の発行した時刻情報を付与し、これら電子署名と時刻情報の組に対して第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証する原本性保証システムである。

【０００８】

これにより、電子化データの原本性保証の際に、第三者機関装置には電子化データが送信されないので、第三者機関装置にアクセスが集中した際にも、第三者機関やその間のネットワークにかかる負荷を低減させることができる。

【０００９】

第２の発明は、電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証する原本性保証システムに関し、前記ユーザ装置に用いられるプログラムであって、前記第１のユーザ装置のコンピュータを、操作者の操作により、電子化データを作成する手段、前記電子化データのうち、前記原本性の保証の対象となる電子化データに対して電子署名を生成する手段、前記電子署名を前記第三者機関装置に送信する手段、として機能させるためのプログラムである。

これにより、第１の発明と同様の作用を奏することができる。

【００１０】

第３の発明は、電子化データに対するユーザ装置の電子署名に対し、自己の電子署名を施して前記電子化データの原本性を保証するための原本性保証ポータルサービスを提供する第三者機関装置と、前記第三者機関装置から提供される原本性保証ポータルサービスをネットワークを介して利用するユーザ装置とからなる原本性保証システムであって、前記第三者機関装置としては、前記ユーザ装置が登録されるテーブルと、前記テーブルに登録されたユーザ装置に対し、予め前記原本性保証ポータルサービスを利用するためのプログラムを提供する手段と、前記プログラムを用いてアクセスされたとき、前記アクセスしてきたユーザ装置のアクセス権限を前記テーブルを参照して確認する手段と、前記アクセス権限の確認されたユーザ装置に対し、前記原本性保証ポータルサービスの利用を許可する手段と、を備えた原本性保証システムである。

これにより、第１の発明と同様な作用を奏する原本性保証システムをネットワークを介したポータルサービスとして実現することができる。

【００１１】

第４の発明は、第３の発明の原本性保証システムにおいて、前記ユーザ装置としては、前記第三者機関装置による電子署名と前記電子化データとを送信する際に、送信先の候補として、前記テーブルの登録内容を前記第三者機関装置に要求する手段と、前記要求に対する応答に基づき、前記テーブルの登録内容をリスト表示する手段と、を備えた原本性保証システムである。

これにより、第３の発明の作用に加え、原本性保証のされた電子化データを送信する際に、送信先の選択を容易に行なうことができる。

【００１２】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照しながら説明する。なお、以下の各実施形態は、公開鍵暗号技術に基づく例であり、第１のユーザ装置ＵＡ、第２のユーザＵＢ、第三者機関ＴＴＰのそれぞれは、自己の公開鍵ペア及び公開鍵証明書を持ち、且つ他者の公開鍵証明書を持っていることを前提とする。

【００１３】

（第１の実施形態）

図１は本発明の第１の実施形態に係る原本性保証システムの構成を示す模式図である。この原本性保証システムは、第１のユーザ装置ＵＡ、第２のユーザ装置ＵＢ及び第三者機関ＴＴＰから構成されている。なお、第１及び第２のユーザ装置ＵＡ，ＵＢは、合計２台以上の不特定多数の台数のうち、任意の２台を例示したものである。

【００１４】

ここで、第１及び第２のユーザ装置ＵＡ，ＵＢは、互いに同一構成であるため、第１又は第２のユーザ装置ＵＡ／ＵＢを例に挙げて述べる。なお、ユーザ装置ＵＡの説明は、添字のＡをＢに置換すると、ユーザ装置ＵＢの説明に置換される。逆も同様である。

【００１５】

ユーザ装置ＵＡは、第三者装置ＴＴＰへの発行要求とその結果の送信に関する発行要求処理部１０Ａと、他のユーザ装置ＵＢからの受信処理とその通知処理に関する受信処理部２０Ａと、第三者装置ＴＴＰの検索に関するＤＢ検索部３０Ａとを備えている。また、各部１０Ａ～３０Ａ，１０Ｂ～３０Ｂは、それぞれハードウェア及び／又はソフトウェアにより実現可能となっている。ソフトウェアにより実現される場合は、例えば記憶媒体又はネットワークから各部１０Ａ～３０Ａ，１０Ｂ～３０Ｂの機能を実現するためのプログラムが予めインストールされた構成となる。

【００１６】

発行要求処理部１０Ａは、記憶部１１Ａ、文書入力部１２Ａ、署名部１３Ａ、発行要求部１４Ａ、応答受信部１５Ａ及びデータ送信部１６Ａを備えている。

【００１７】

記憶部１１Ａは、自装置ＵＡの識別情報Ａと、自装置ＵＡの公開鍵ペア及び公開鍵証明書と、他装置ＵＢ，ＴＴＰの公開鍵証明書と、文書入力部１２から入力される電子化文書Ｄと、電子化文書の識別情報$ＩＤ_{A,D}$と、署名部１３により作成された電子署名$Ｓ_{A}$（Ｄ）と、第三者装置ＴＴＰに作成された識別情報$ＩＤ_{TTP}$

$_{A,D}$、登録日時$date_{TTP,D}$、電子署名S_{TTP}（$ID_{TTP,D}$、S_A（D）、$date_{TTP,D}$）とが記憶されるものである。

【００１８】

なお、記憶内容の添字のＡは、ユーザ装置ＵＡにより作成されたことを示し（例、$ID_{A,D}$、S_A（D））、記憶内容の添字のＴＴＰは、第三者機関ＴＴＰにより作成されたことを示す（例、$ID_{TTP,D}$、$date_{TTP,D}$、S_{TTP}（…略…））。また、添字のＤは、対応する電子化文書Ｄを示しているので、電子化文書の識別情報$ID_{A,D}$又は$ID_{TTP,D}$としてもよい。また、電子化データとしての電子化文書Ｄは、文字列からなる文章のみの電子化された文書データに限らず、数表等のデータ又は画像データを含む文書、あるいはこれらの組合せからなる文書でもよく、そのデータ形式及びデータ量は任意のものが使用可能となっている。例えば音声データを含む文書としてもよく、また少ないデータ量であってもよい。

【００１９】

文書入力部１２Ａは、操作者の操作により、電子化文書Ｄを作成、修正又は編集し、得られた電子化文書Ｄを記憶部１１Ａに書込む機能をもっている。

【００２０】

署名部１３Ａは、操作者の操作により、記憶部１１Ａ内の対象となる電子化文書Ｄに対し、自己の秘密鍵を用いて電子署名S_A（D）を生成する機能と、生成した電子署名S_A（D）を記憶部１１Ａに書込む機能とをもっている。

【００２１】

発行要求部１４Ａは、記憶部１１Ａの内容に基づいて原本性保証データの発行要求を作成する機能と、この発行要求を第三者機関ＴＴＰに送信する機能とをもっている。

【００２２】

ここで、発行要求は、例えば、要求元（ユーザ装置ＵＡ）を示す要求者情報Ａ、電子化文書Ｄのユーザ装置ＵＡによる電子署名S_A（D）、ユーザ装置ＵＡにおける電子化文書Ｄの識別情報$ID_{A,D}$を含んでいる。すなわち、発行要求は、{A、S_A（D）、$ID_{A,D}$}からなるデータである。なお、識別情報$ID_{A,D}$は、省略してもよいが、使用されることが処理効率向上の観点から望ましい。

【００２３】

応答受信部１５Ａは、第三者機関ＴＴＰから受けた応答データを記憶部１１Ａに書込む機能をもっている。

【００２４】

データ送信部１６Ａは、操作者の操作又は応答受信部１５Ａからの制御により、記憶部１１Ａを参照し、識別情報$ID_{A,D}$により特定される電子化文書Ｄと、応答データから$ID_{A,D}$を除いてＡ，S_A（Ｄ）を付加したデータ（＝要求側登録データ）とを含む保証済みデータ｛Ｄ、Ａ，S_A（Ｄ）、$ID_{TTP,D}$、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝をユーザ装置ＵＢに送信する機能をもっている。

【００２５】

次に、受信処理部２０Ａ，２０Ｂについて説明する。なお、後述する動作説明中では、ユーザ装置ＵＢの受信処理部２０Ｂの動作が述べられるので、混乱を避けるため、ここではユーザ装置ＵＢの受信処理部２０Ｂを例に挙げて説明する。

【００２６】

ユーザ装置ＵＢの受信処理部２０Ｂは、改ざん検証部２１Ｂ、保証確認部２２Ｂ、受信通知部２３Ｂ及び確認部２４Ｂを備えている。

【００２７】

改ざん検証部２１Ｂは、他のユーザ装置ＵＡから保証済みデータを受けると、保証済みデータ内の識別情報Ａに対応する公開鍵証明書を用いて電子署名S_A（Ｄ）を用いて、電子化文書Ｄの改ざんの有無を検証する機能をもっている。

【００２８】

保証確認部２２Ｂは、改ざん検証部２１Ｂによる検証の結果、電子化文書Ｄに改ざんが無いとき、記憶部１１Ｂ内の第三者機関ＴＴＰの公開鍵証明書を用いて原本性保証データS_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）を復号し、復号結果とデータS_A（Ｄ）、$ID_{TTP,D}$、$date_{TTP,D}$とを比較することにより、第三者機関ＴＴＰにより原本性が保証された旨を確認する機能をもっている。なお、原本性保証の確認は、改ざんの有無の検証よりも前に行なっても良い。

【００２９】

受信通知部２３Ｂは、改ざん検証部２１Ｂによる改ざん無しの検証と保証確認部２２Ｂによる原本性保証の確認とが完了した後、受信否認防止のための受信通知を作成し、この受信通知｛Ｂ、$ID_{TTP,D}$、$date_{B,D}$、S_B（S_A（Ｄ），$date_{B,D}$）｝を第三者機関ＴＴＰに送信する機能をもっている。

【００３０】

受信通知は、例えば、受信者（ユーザ装置ＵＢ）の識別情報Ｂ、第三者機関ＴＴＰが電子化文書Ｄに付与した識別情報$ID_{TTP,D}$、ユーザ装置ＵＢでの受信日時$date_{B,D}$、ユーザ装置ＵＢの受信を証明（受信否認を防止）するための情報S_B（S_A（Ｄ），$date_{B,D}$）を含んでいる。

【００３１】

確認部２４Ｂは、第三者機関ＴＴＰから受信確認を受信すると、$ID_{TTP,D}$をキーにして、ユーザ装置ＵＡから受信した電子化文書Ｄを検索し、受信通知を第三者機関ＴＴＰが正しく処理できた旨を確認する機能をもっている。

【００３２】

受信確認は、例えば、第三者機関ＴＴＰが電子化文書Ｄに付与した識別情報$ID_{TTP,D}$、ＢのＡからの受信日時$date_{B,D}$、ユーザ装置ＵＢからの受信通知を証明する情報S_{TTP}（S_B（Ｄ），$date_{B,D}$）を含んでいる。なお、受信日時$date_{B,D}$は、ユーザ装置ＵＢが保存する前提であれば省略してもよい。

【００３３】

ＤＢ検索部３０Ａは、操作者の操作により、識別情報$ID_{TTP,D}$をキーにして第三者機関ＴＴＰの原本性保証ＤＢを検索し、その登録内容を入手する機能をもっている。

【００３４】

一方、第三者機関ＴＴＰは、原本性保証ＤＢ（data base）４０、要求側登録部４１及び受信側登録部４２を備えている。

【００３５】

原本性保証ＤＢ４０は、要求側登録部４１及び受信側登録部４２により、要求側登録データ｛$ID_{TTP,D}$、Ａ、S_A（Ｄ）、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝及び受信側登録データ｛Ｂ、$date_{B,D}$、S_B（S_A（Ｄ），da

$te_{B,D}$）｝が識別情報$ID_{TTP,D}$をキーにして登録されるものであり、登録内容が各ユーザ装置ＵＡ，ＵＢのＤＢ検索部３０により検索可能となっている。

【００３６】

要求側登録部４１は、ユーザ装置ＵＡから発行要求を受けると、この発行要求に基づいて要求側登録データ｛$ID_{TTP,D}$、Ａ、S_A（Ｄ）、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝を作成する機能と、作成した要求側登録データを原本性保証ＤＢに登録する機能と、登録した要求側登録データからＡ，S_A（Ｄ）を除いて$ID_{A,D}$を付加した応答データ｛$ID_{A,D}$、$ID_{TTP,D}$、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝をユーザ装置ＵＡに送信する機能とをもっている。

【００３７】

ここで、要求側登録データは、例えば、第三者機関ＴＴＰにおける電子化文書Ｄの識別情報$ID_{TTP,D}$、要求者（ユーザ装置ＵＡ）の識別情報Ａ、要求者による電子署名S_A（Ｄ）、第三者機関ＴＴＰによる原本性保証の処理の日時$date_{TTP,D}$、と、これら$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$を連接した連接データに対する第三者機関ＴＴＰの電子署名としての原本性保証データS_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）を含んでいる。すなわち、要求側登録データは、｛$ID_{TTP,D}$、Ａ、S_A（Ｄ）、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝である。

【００３８】

受信側登録部４２は、ユーザ装置ＵＢから受信通知を受けると、この受信通知及び原本性保証ＤＢ中の$ID_{TTP,D}$に基づいて、受信側登録データ｛Ｂ、$date_{B,D}$、S_B（S_A（Ｄ），$date_{B,D}$）｝を識別情報$ID_{TTP,D}$に対応付けて追加的に原本性保証ＤＢに登録する機能と、この登録の後、受信確認｛$ID_{TTP,D}$、$date_{B,D}$、S_{TTP}（S_B（Ｄ），$date_{B,D}$）｝をユーザ装置ＵＢに送信する機能とをもっている。

【００３９】

次に、以上のように構成された原本性保証システムの動作を図２の模式図及び図３のフローチャートを用いて説明する。なお、図２の模式図は、ユーザ装置Ｕ

Ａを送信側とし、ユーザ装置ＵＢを受信側としたときの各ユーザ装置ＵＡ，ＵＢにおいて必要な機能ブロックのみを図示しており、送信側にとっての受信処理部２０Ａや受信側にとっての発行要求処理部１０Ｂは夫々図示を省略している。

【００４０】

さてユーザ装置ＵＡにおいては、文書入力部１２Ａが、操作者の操作により、電子化文書Ｄを作成、修正又は編集し、得られた電子化文書Ｄを記憶部１１Ａに書込んだとする。

【００４１】

ここで、ユーザ装置ＵＡにおいては、電子化文書の原本性保証が必要な場合、ユーザ装置ＵＢに文書を送信する前に、操作者の操作により、署名部１３Ａが、記憶部１１Ａ内の対象となる電子化文書Ｄに対し、自己の秘密鍵を用いて電子署名ＳＡ（Ｄ）を生成し、この電子署名ＳＡ（Ｄ）を記憶部１１Ａに書込む。

【００４２】

また、発行要求部１４Ａが、記憶部１１Ａの内容に基づいて電子化文書Ｄの原本性保証データの発行要求｛Ａ、S_A（Ｄ）、$ID_{A,D}$｝を作成し、得られた発行要求を第三者機関ＴＴＰに送信する（ＳＴ１）。

【００４３】

第三者機関ＴＴＰでは、発行要求を受けると、要求側登録部４１が、この発行要求に基づいて要求側登録データ｛$ID_{TTP,D}$、Ａ、S_A（Ｄ）、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝を作成し、得られた要求側登録データを原本性保証ＤＢ４０に登録する（ＳＴ２）。

【００４４】

次に、要求側登録部４１は、ユーザ装置ＵＡに対し、要求側登録データからＡ，S_A（Ｄ）を除いて$ID_{A,D}$を付加した応答データ｛$ID_{A,D}$、$ID_{TTP,D}$、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝をユーザ装置ＵＡに送信する（ＳＴ３）。なお、応答データとしては、$ID_{A,D}$に代えて、S_A（Ｄ）を用いてもよい。

【００４５】

ユーザ装置ＵＡでは、応答データを受けると、応答受信部１５Ａがこの応答デ

ータを記憶部１１Ａに書込む。また、データ送信部１６Ａが、操作者の操作又は応答受信部１５Ａからの制御により、記憶部１１Ａを参照し、識別情報$ID_{A,D}$により特定される電子化文書Ｄと、応答データから$ID_{A,D}$を除いてＡ，S_A（Ｄ）を付加したデータ（＝要求側登録データ）とを含む保証済みデータ｛Ｄ、Ａ，S_A（Ｄ）、$ID_{TTP,D}$、$date_{TTP,D}$、S_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）｝をユーザ装置ＵＢに送信する（ＳＴ４）。なお、電子化文書Ｄは必要により暗号化してもよい。

【００４６】

ユーザ装置ＵＢでは、保証済みデータを受けると、改ざん検証部２１Ｂが、保証済みデータ内の識別情報Ａに対応する公開鍵証明書を用いて電子署名S_A（Ｄ）を用いて、電子化文書Ｄの改ざんの有無を検証する。

【００４７】

ここで、電子化文書Ｄに改ざんが無いとき、ユーザ装置ＵＢでは、保証確認部２２Ｂが、第三者機関ＴＴＰの公開鍵証明書を用いて原本性保証データS_{TTP}（$ID_{TTP,D}$、S_A（Ｄ）、$date_{A,D}$）を復号し、復号結果とデータS_A（Ｄ）、$ID_{TTP,D}$、$date_{TTP,D}$とを比較することにより、第三者機関ＴＴＰが原本性を保証したことを確認する。

【００４８】

さて、原本性保証の確認の後、ユーザ装置ＵＢでは、受信通知部２３Ｂが、受信否認防止のための受信通知を作成し、この受信通知｛Ｂ、$ID_{TTP,D}$、$date_{B,D}$、S_B（S_A（Ｄ），$date_{B,D}$）｝を第三者機関ＴＴＰに送信する（ＳＴ５）。

【００４９】

第三者機関ＴＴＰでは、受信通知を受けると、受信側登録部４２が原本性保証ＤＢ中の$ID_{TTP,D}$に基づいて、受信側登録データ｛Ｂ、$date_{B,D}$、S_B（S_A（Ｄ），$date_{B,D}$）｝を識別情報$ID_{TTP,D}$に対応付けて追加的に原本性保証ＤＢに登録する（ＳＴ６）。

【００５０】

しかる後、第三者機関ＴＴＰでは、受信側登録部４２が受信確認｛$ID_{TTP,D}$、$date_{B,D}$、S_{TTP}（S_B（Ｄ），$date_{B,D}$）｝をユーザ装置ＵＢに送信する（ＳＴ

７）。

【００５１】

ユーザ装置ＵＢでは、受信確認を受信すると、確認部２４Ｂが、$ID_{TTP,D}$をキーにして、ユーザ装置ＵＡから受信した電子化文書Ｄを検索し、受信通知を第三者機関ＴＴＰが正しく処理できた旨を確認する。

【００５２】

以上により、ユーザ装置ＵＡに関し、ユーザ装置ＵＢに対する電子化文書の原本性保証と受信否認防止の処理が完了する。

【００５３】

以後、ユーザ装置ＵＡがユーザ装置ＵＢの受信を確認したい場合、例えば第三者機関ＴＴＰの提供するＷＷＷサービスなどにより、ユーザ装置ＵＡ内のＤＢ検索部３０Ａが$ID_{TTP,D}$をキーにして原本性保証ＤＢを検索することにより、原本性保証及び／又は受信を確認することができる。

【００５４】

また、この後、必要により、ユーザ装置ＵＡとユーザ装置ＵＢとの役割を交替し、ユーザ装置ＵＢが作成した電子化文書Ｄ’に関し、前述同様に、電子化文書Ｄ’の原本性保証と、ユーザ装置ＵＡに対する受信否認防止との処理をそれぞれ行なってもよい。すなわち、第１及び第２のユーザ装置ＵＡ，ＵＢは、電子化文書の交換により取引き等を行なう場合、電子化文書を授受する毎に、互いに役割を交替して原本性保証と受信否認防止を行なうようにしてもよい。

【００５５】

上述したように本実施形態によれば、電子化文書Ｄの原本性保証の際に、第三者機関ＴＴＰには電子化文書Ｄが送信されず、Ｄよりも情報の少ない電子署名が送信されるので、第三者機関ＴＴＰにアクセスが集中した際の第三者機関又はその間のネットワークにかかる負荷を低減させることができる。

【００５６】

また、原本性保証ＤＢ４０に要求側登録データ及び受信側登録データを登録するので、各ＤＢ検索部３０Ａ，３０Ｂは、後日（ＳＴ７の後）あるいは処理途中（例、ＳＴ４とＳＴ５との間）でも必要により、原本性保証ＤＢ４０の登録内容

を確認することができる。

【００５７】

また、この確認により何らかの立証を行なうことができる。例えば、登録日時$date_{TTP,D}$と、受信日時$date_{B,D}$との差を見ることにより、ユーザ装置ＵＡの処理の遅れの有無を立証することができる。

【００５８】

（第２の実施形態）

図４は本発明の第２の実施形態に係る原本性保証ポータルサービスの構成を示す模式図である。この原本性保証ポータルサービスは、契約により、第１の実施形態の機能を実現するプログラムを第三者機関ＴＴＰが各ユーザ装置ＵＡ，ＵＢに提供して実施可能とする方式である。

【００５９】

このユーザ装置ＵＡ，ＵＢに提供されるプログラムは、前述した発行要求処理部１０Ａ，１０Ｂ、受信処理部２０Ａ，２０Ｂ及びＤＢ検索部３０Ａ，３０Ｂの機能を実現するための、発行要求プログラム１０Ａ*，１０Ｂ*、受信処理プログラム２０Ａ*，２０Ｂ*、ＤＢ検索プログラム３０Ａ*，３０Ｂ*と、送信先の選択処理を実現するための選択プログラム５０Ａ*，５０Ｂ*とである。なお、この選択プログラム５０Ａ*，５０Ｂ*は、発行要求処理部１０Ａ，１０Ｂに関するプログラム１０Ａ*，１０Ｂ*に組み込まれている。

【００６０】

なお、契約の際に、各契約者の各ユーザ装置ＵＡ，ＵＢは、自装置ＵＡ，ＵＢの識別情報Ａ，Ｂ、自装置ＵＡ，ＵＢの公開鍵証明書P_A，P_B、自装置ＵＡ，ＵＢのアドレス情報ADR_A，ADR_B及び自装置ＵＡ，ＵＢのデータ通信プロトコル（例、ｓｍｔｐ、ｈｔｔｐ（ｓ）、ｆｔｐ（ｓ））を第三者機関ＴＴＰに提供することを前提とする。

【００６１】

第三者機関ＴＴＰは、図５に示すように、これらの提供された情報を各ユーザ装置ＵＡ，ＵＢ毎にテーブル６０に記憶しており、各ユーザ装置ＵＡ，ＵＢからの要求により、テーブル６０の内容を契約者の一覧として要求元のユーザ装置Ｕ

Ａ，ＵＢに提供する機能をもっている。

【００６２】

また、契約の後、クライアント装置としての各ユーザ装置ＵＡ，ＵＢは、他のユーザ装置ＵＢ，ＵＡから文書やデータを受信可能なように、サーバ装置としての第三者機関ＴＴＰにログイン可能な状態にあることを前提とする。

【００６３】

すなわち、契約の後、各ユーザ装置ＵＡ，ＵＢは、図６（ａ），（ｂ）に示すように、少なくとも第三者機関ＴＴＰの識別情報ＴＴＰと公開鍵証明書P_{TTP}とアドレス情報ADR_{TTP}とデータ通信プロトコルとをテーブルＴＡ，ＴＢに保持し、適宜、他のユーザ装置ＵＢ，ＵＡの識別情報Ｂ，Ａと公開鍵証明書P_B，P_Aとアドレス情報ADR_B，ADR_Aとデータ通信プロトコルとをもテーブルＴＡ，ＴＢに保持した状態にある。

【００６４】

一方、第三者機関ＴＴＰは、テーブル６０を参照して各ユーザ装置ＵＡ，ＵＢのアクセス権限を確認可能な状態にあり、アクセス権限の確認されたユーザ装置に対し、原本性保証ポータルサービスの利用を許可する機能をもっている。

【００６５】

次に、以上のように構成された原本性保証ポータルサービスの動作を説明する。

【００６６】

原本性保証ポータルサービスでは、図７に示すように、第三者機関ＴＴＰに対し、前述したステップＳＴ１～ＳＴ４に対応する登録サービスＰＳ１と、前述したステップＳＴ５～ＳＴ７に対応する受信確認サービスＰＳ２と、前述したＤＢ検索部３０Ａ，３０ＢによるＤＢ検索に対応する原本性確認サービスＰＳ３とが選択的に実行要求可能となっている。但し、各サービスの実行は、第三者機関ＴＴＰがテーブル６０を参照し、実行要求したユーザ装置のアクセス権限を確認した後である。

【００６７】

例えばユーザ装置ＵＡでは登録サービスＰＳ１を選択すると、第三者機関ＴＴ

Ｐによるアクセス権限の確認により、登録サービスＰＳ１の利用が許可された後、前述したステップＳＴ１～ＳＴ３に相当する処理が第三者機関ＴＴＰとの間で実行される。この処理が完了した後、ユーザ装置ＵＡでは、送信先の選択プログラム５０Ａ＊が起動され、送信先の選択処理が実行される。

【００６８】

ユーザ装置ＵＡでは、この選択処理の実行に伴い、テーブル６０に登録された契約者の一覧を第三者機関ＴＴＰに要求し、その応答に基づいて、第三者機関ＴＴＰと契約中の契約者（例、企業、個人）の一覧を表示する。

【００６９】

ここで、ユーザ装置ＵＡの操作者が一覧内の契約者を送信先として選択すると、送信先のユーザ装置ＵＢに対し、所定のデータ通信プロトコルが起動されてユーザ装置ＵＢに送信可能な状態となる。

【００７０】

例えばデータ通信プロトコルがｓｍｔｐの場合、メイラが起動され送信先のアドレスがユーザ装置ＵＢのアドレスで埋められる。ｈｔｔｐ（ｓ）の場合、送信先のユーザ装置ＵＢのホームページが表示される。ｆｔｐ（ｓ）の場合、ｆｔｐ（ｓ）クライアントが立ち上がって送信先のユーザ装置ＵＢに接続される。

【００７１】

ユーザ装置ＵＡは、前述したステップＳＴ４で送信する保証済みデータを作成し、保証済みデータを選択したデータ通信プロトコルによりユーザ装置ＵＢに送信する。これにより、登録サービスＰＳ１が完了する。

【００７２】

受信側のユーザ装置ＵＢは、受信確認サービスＰＳ２を選択すると、第三者機関ＴＴＰによるアクセス権限の確認の後、前述したステップＳＴ５～ＳＴ７に相当する処理を第三者機関ＴＴＰと協調しながら自動処理する。自動処理の後、受信確認サービスＰＳ２が完了する。

【００７３】

これにより、第１の実施形態と同様に、原本性保証と受信否認防止とを実現することができる。

【００７４】

また、ユーザ装置ＵＡは、原本性確認サービスＰＳ３を選択すると、第三者機関ＴＴＰによるアクセス権限の確認の後、電子化文書Ｄの識別情報ＩＤTTP,Dを第三者機関ＴＴＰに対して提示し、原本性保証ＤＢ４０から電子署名S_A（Ｄ）を取り寄せる処理と、この電子署名ＳＡ（Ｄ）に基づいて、電子化文書Ｄの原本性を確認する処理とを実行する。これにより、原本性確認サービスＰＳ３が完了する。

【００７５】

上述したように本実施形態によれば、第１の実施形態と同様の作用効果をもつ原本性保証サービスを、ネットワークを介したポータルサービスとして実現することができる。また、原本性保証のされた電子化文書を送信する際に、送信先の選択を容易に行なうことができる。

【００７６】

なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【００７７】

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【００７８】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【００７９】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【００８０】

また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【００８１】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【００８２】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【００８３】

なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【００８４】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【００８５】

【発明の効果】

以上説明したように本発明によれば、第三者機関やその間のネットワークにかかる負荷を低減させることができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係る原本性保証システムの構成を示す模式図

【図２】

同実施形態における原本性保証システムの動作を説明するための模式図

【図３】

同実施形態における動作を説明するためのフローチャート

【図４】

本発明の第２の実施形態に係る原本性保証ポータルサービスの構成を示す模式図

【図５】

同実施形態における第三者機関側のテーブルの内容を示す模式図

【図６】

同実施形態におけるユーザ装置側のテーブルの内容を示す模式図

【図７】

同実施形態における動作を説明するための模式図

【符号の説明】

ＵＡ，ＵＢ…ユーザ装置

ＴＴＰ…第三者機関

１０Ａ，１０Ｂ…発行要求処理部

１０Ａ＊，１０Ｂ＊…発行要求プログラム

１１Ａ，１１Ｂ…記憶部

１２Ａ，１２Ｂ…文書入力部

１３Ａ，１３Ｂ…署名部

１４Ａ，１４Ｂ…発行要求部

１５Ａ，１５Ｂ…応答受信部

１６Ａ，１６Ｂ…データ送信部

２０Ａ，２０Ｂ…受信処理部

２０Ａ＊，２０Ｂ＊…受信処理プログラム

２１Ａ，２１Ｂ…改ざん検証部

２２Ａ，２２Ｂ…保証確認部

２３Ａ，２３Ｂ…受信通知部

２４Ａ，２４Ｂ…確認部

３０Ａ，３０Ｂ…ＤＢ検索部

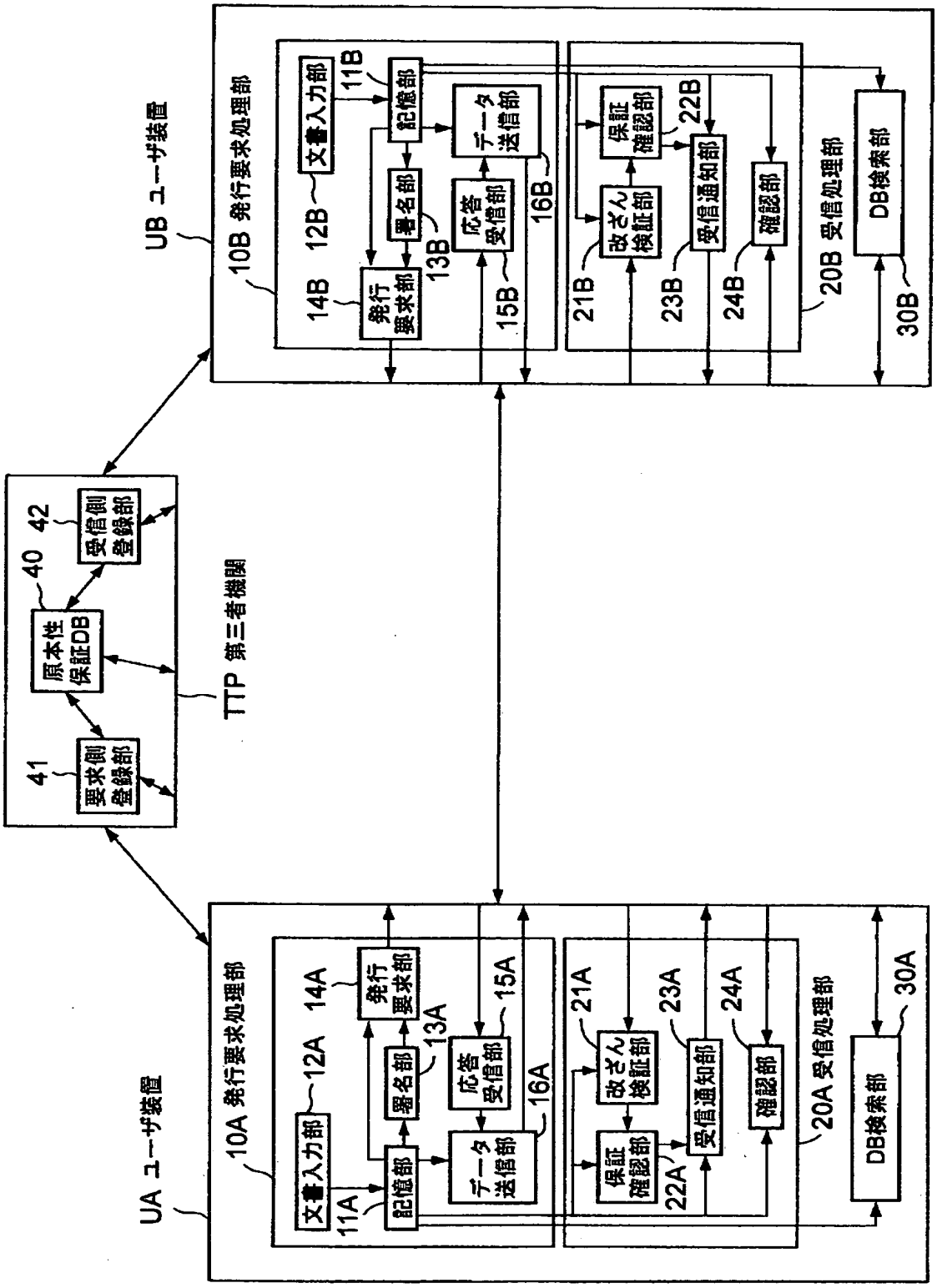
３０Ａ*，３０Ｂ*…ＤＢ検索プログラム

５０Ａ*，５０Ｂ*…選択プログラム

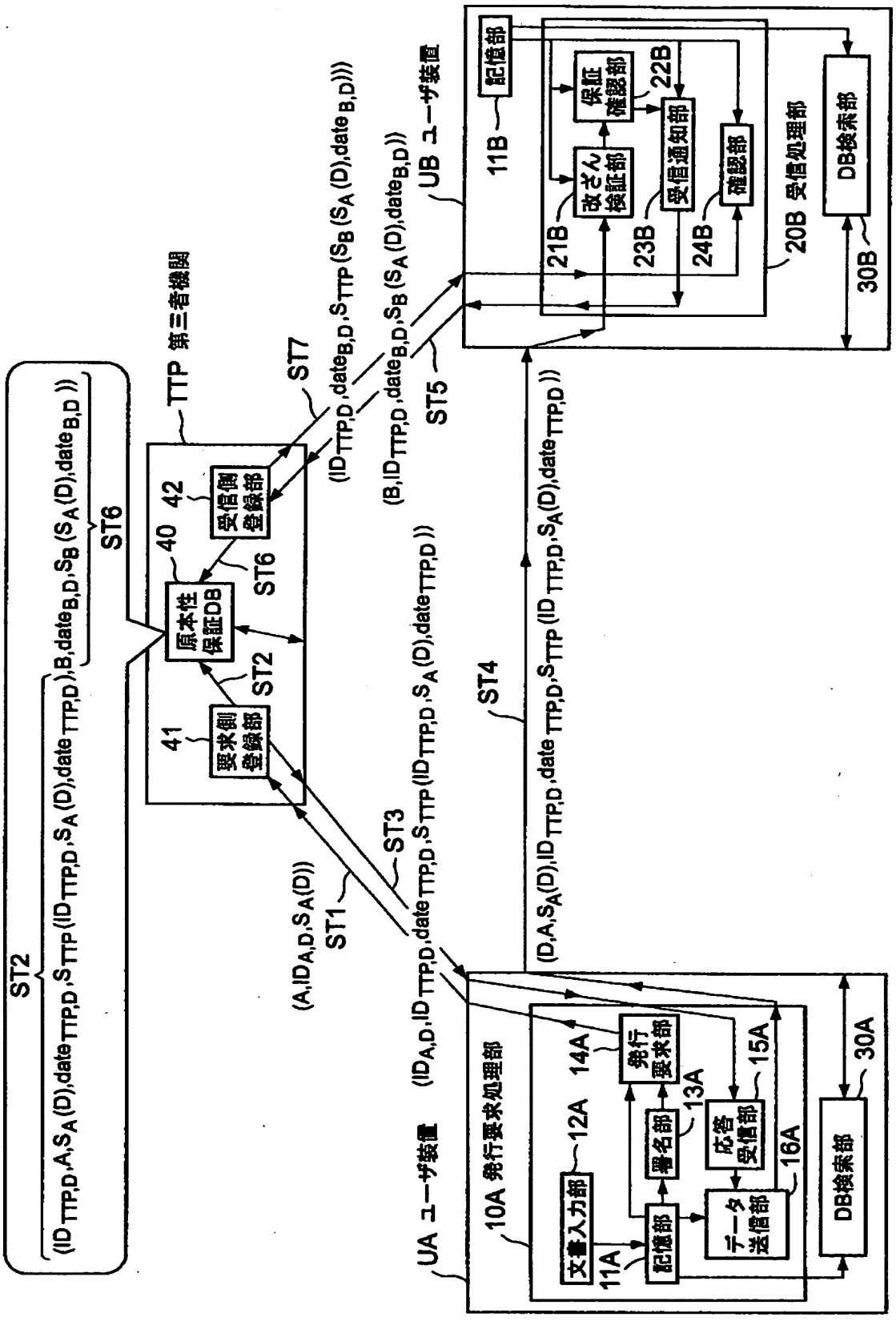
６０，ＴＡ，ＴＢ…テーブル

【書類名】　図面

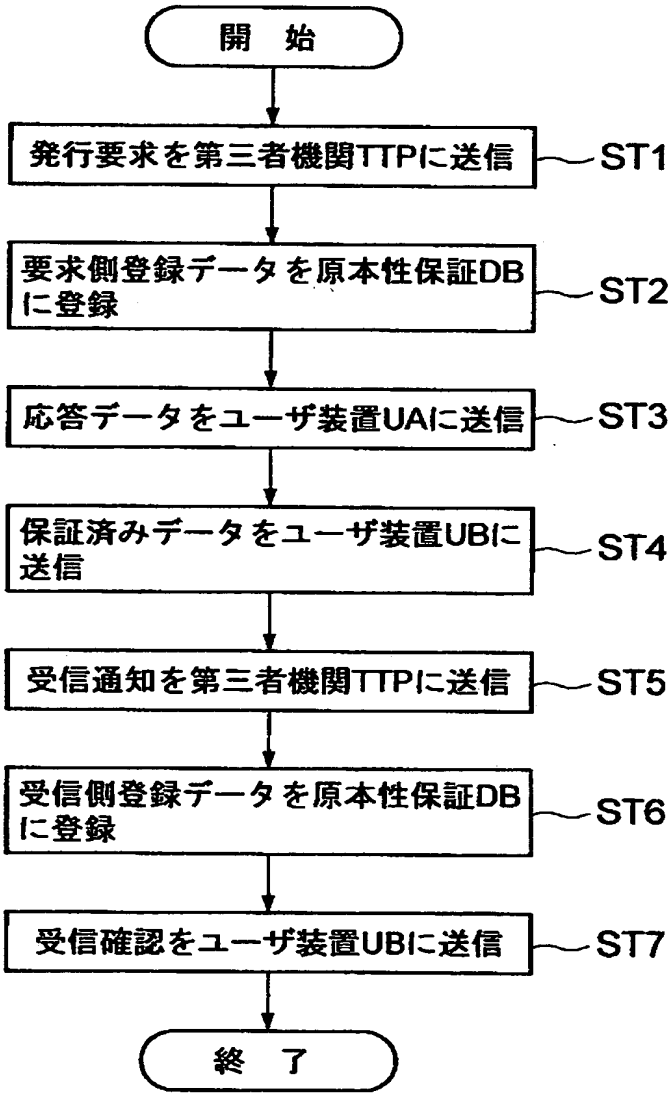
【図１】


UB ユーザ装置
10B 発行要求処理部
文書入力部
11B
記憶部
12B
署名部
13B
発行要求部
14B
データ送信部
16B
応答受信部
15B
保証確認部
22B
改ざん検証部
21B
受信通知部
23B
確認部
24B
20B 受信処理部
DB検索部
30B
TTP 第三者機関
受信側登録部
42
原本性保証DB
40
要求側登録部
41
UA ユーザ装置
10A 発行要求処理部
文書入力部
11A
記憶部
12A
署名部
13A
発行要求部
14A
データ送信部
16A
応答受信部
15A
保証確認部
22A
改ざん検証部
21A
受信通知部
23A
確認部
24A
20A 受信処理部
DB検索部
30A

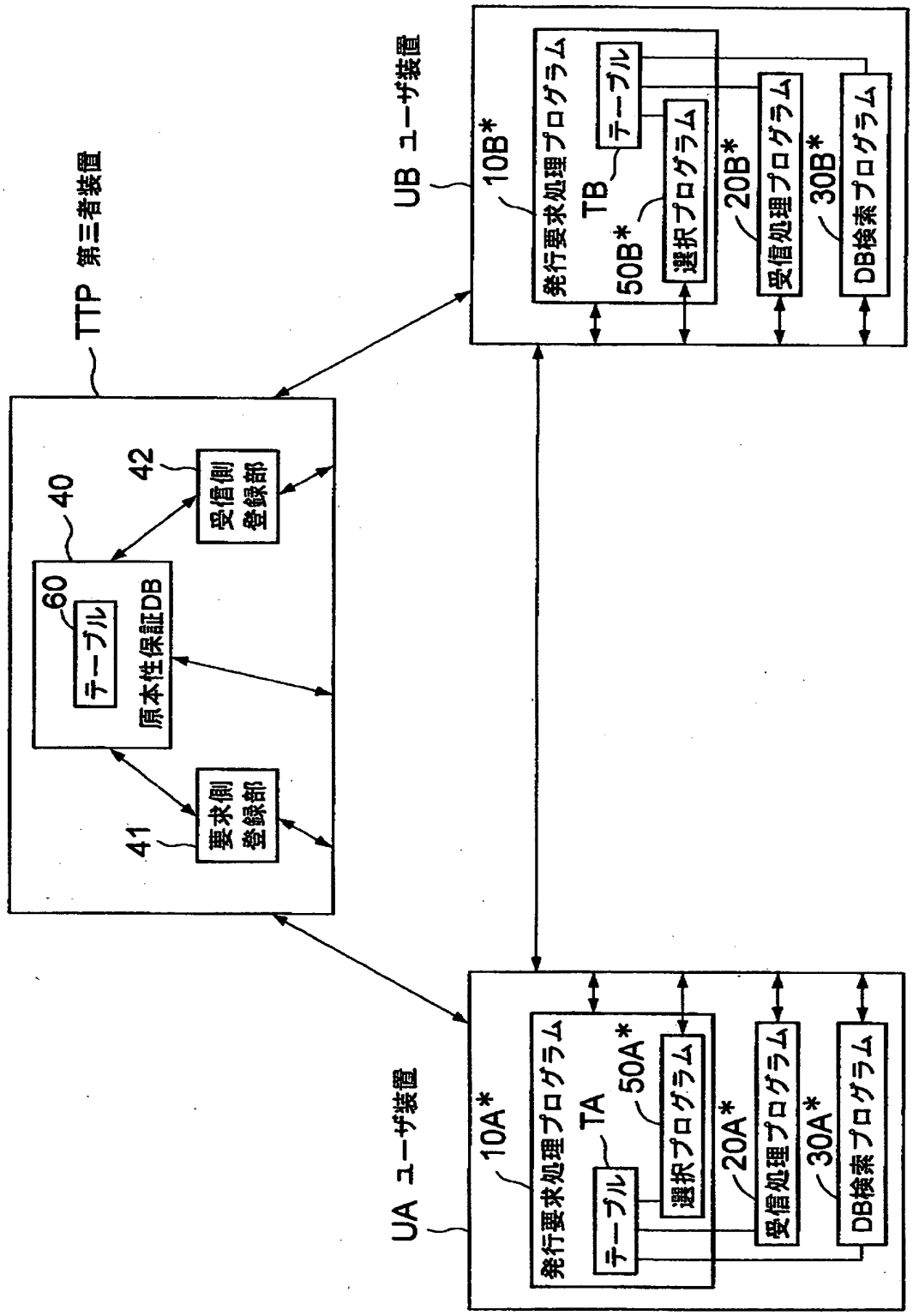
【図２】


TTP 第三者機関
UA ユーザ装置
UB ユーザ装置
10A 発行要求処理部
20B 受信処理部
30A
30B
40
41
42
11A
11B
12A
13A
14A
15A
16A
21B
22B
23B
24B
原本性保証DB
要求側登録部
受信側登録部
文書入力部
記憶部
署名部
発行要求部
データ送信部
応答受信部
DB検索部
改ざん検証部
保証確認部
受信通知部
確認部
ST1
ST2
ST3
ST4
ST5
ST6
ST7
(A,ID_A,D,S_A(D))
(ID_A,D,ID_TTP,D,date_TTP,D,S_TTP(ID_TTP,D,S_A(D),date_TTP,D))
(ID_TTP,D,A,S_A(D),date_TTP,D,S_TTP(ID_TTP,D,S_A(D),date_TTP,D),B,date_B,D,S_B(S_A(D),date_B,D))
(D,A,S_A(D),ID_TTP,D,date_TTP,D,S_TTP(ID_TTP,D,S_A(D),date_TTP,D))
(B,ID_TTP,D,date_B,D,S_B(S_A(D),date_B,D))
(ID_TTP,D,date_B,D,S_TTP(S_B(S_A(D),date_B,D)))
ST6

【図３】


開　始
発行要求を第三者機関TTPに送信
ST1
要求側登録データを原本性保証DBに登録
ST2
応答データをユーザ装置UAに送信
ST3
保証済みデータをユーザ装置UBに送信
ST4
受信通知を第三者機関TTPに送信
ST5
受信側登録データを原本性保証DBに登録
ST6
受信確認をユーザ装置UBに送信
ST7
終　了

【図４】


TTP 第三者装置
40
60
テーブル
原本性保証DB
42
受信側登録部
41
要求側登録部
UB ユーザ装置
10B*
発行要求処理プログラム
TB
テーブル
50B*
選択プログラム
20B*
受信処理プログラム
30B*
DB検索プログラム
UA ユーザ装置
10A*
発行要求処理プログラム
TA
テーブル
50A*
選択プログラム
20A*
受信処理プログラム
30A*
DB検索プログラム

【図５】

60

A	P_A	ADR_A	ftp
B	P_B	ADR_B	smtp
⋮	⋮	⋮	⋮

【図６】

(a)

TA

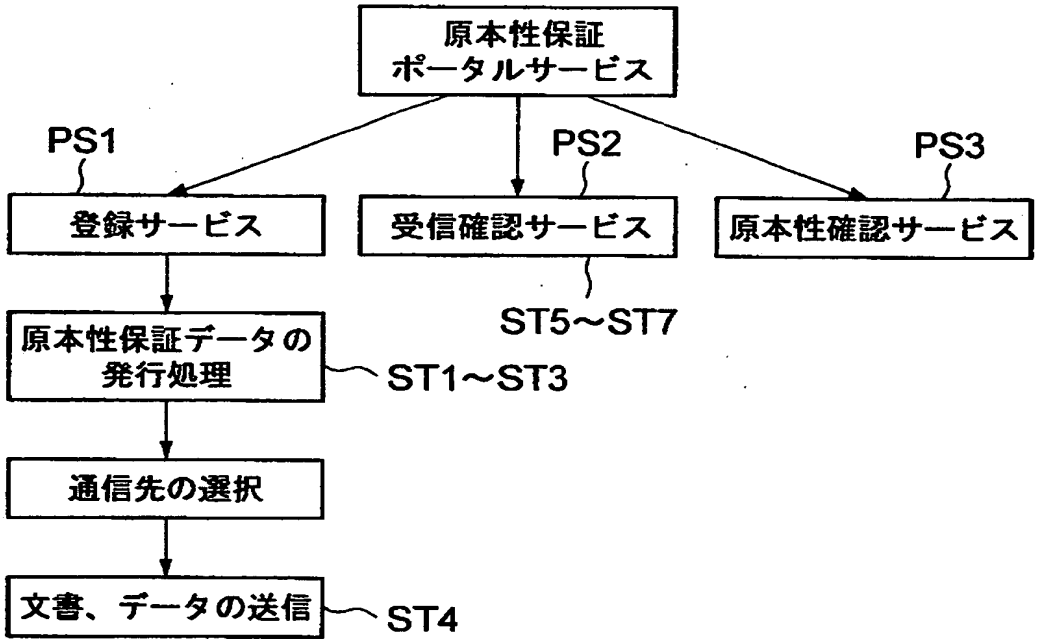
TTP	P_{TTP}	ADR_{TTP}	ftp
B	P_B	ADR_B	smtp
⋮	⋮	⋮	⋮

(b)

TB

TTP	P_{TTP}	ADR_{TTP}	ftp
A	P_A	ADR_A	ftp
⋮	⋮	⋮	⋮

【図７】


原本性保証
ポータルサービス
PS1
PS2
PS3
登録サービス
受信確認サービス
原本性確認サービス
ST5～ST7
原本性保証データの
発行処理
ST1～ST3
通信先の選択
文書、データの送信
ST4

【書類名】　　要約書

【要約】

【課題】　第三者機関やその間のネットワークにかかる負荷を低減させる。

【解決手段】　電子化文書Ｄに対するユーザ装置ＵＡの電子署名S_A（Ｄ）に対し、第三者機関ＴＴＰの発行した時刻情報$date_{TTP}$を付与し、これら電子署名と時刻情報の組に対して第三者機関の電子署名を施すことにより、電子化文書の原本性を保証する。これによれば、電子化文書の原本性保証の際に、第三者機関装置には電子化文書が送信されないので、第三者機関装置にアクセスが集中した際にも、第三者機関やその間のネットワークにかかる負荷を低減できる。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝

２．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　東京都港区芝浦一丁目１番１号
氏　名　株式会社東芝